REFERENCE GUIDE – RISK CALCULATION METHODOLOGY

BACKGROUND

This guide provides an explanation of the underlying calculations that drive GuardianERM's risk-based methodology. In this reference guide we will cover the following:

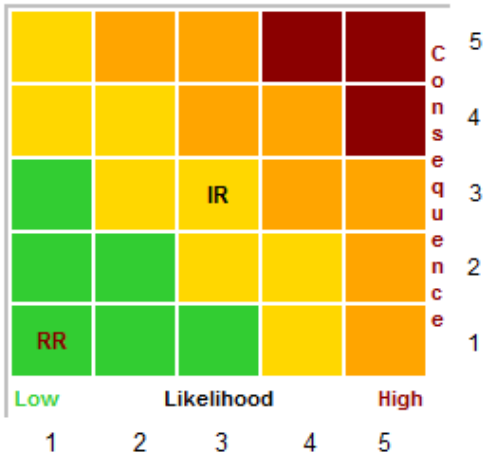
1. How Inherent Risk **(IR)** is initially rated and represented on the heat map configuration
2. How attached Controls affect risk ratings
3. How the Residual Risk **(RR)** is determined once control effectiveness is input
4. How to manually override the RR if necessary

CALCULATING THE INHERENT RISK

The inherent risk represents the level of risk before any mitigating controls are applied. It is calculated by combining the ratings for the ***likelihood*** and ***consequence,*** each measured on a five-point scale:

Scale	Likelihood	Consequence
1	Rare	Insignificant
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost Certain	Catastrophic

For example, if a risk is rated 3 (Possible) for Likelihood and 3 (Moderate) for Consequence, the overall inherent risk sits in the middle of the heat map accordingly.



✓ **TIP:** Administrators can configure the heat map to reflect their organisations risk appetite – adjusting colours and terminology as needed.

CONTROLS EFFECTIVENESS RATINGS

Once an initial risk assessment is complete, controls can be added to reduce the likelihood or consequence of a risk. Each control will have two measures:

- ***Effectiveness Likelihood*** is how well the control reduces the chance of occurrence
- ***Effectiveness Consequence*** is how well the control reduces the severity of impact

When an attached controls effectiveness rating is applied, a score is automatically generated based on the qualitative rating of each control. The equivalent quantitative score for each rating is as follows (system default):

Level	Effectiveness	% Equivalent
0	Not Effective	0%
1	Slightly Effective	20%
2	Somewhat Effective	40%
3	Reasonably Effective	60%
4	Mostly Effective	80%
5	Very Effective	100%

When multiple controls are attached to the same risk, the system assumes the controls work independently. Thus, the combined effectiveness is calculated using the formula for probability of at least one success:

$$\textit{Combined Effectiveness} = 1 - [\,(1 - p_1) \times (1 - p_2) \times (1 - p_3) \ldots]$$

Where p_1, p_2, p_3…. Are the effectiveness values (%) of each control. This means that additional controls increase total effectiveness, but with diminishing returns.

Why this Methodology?

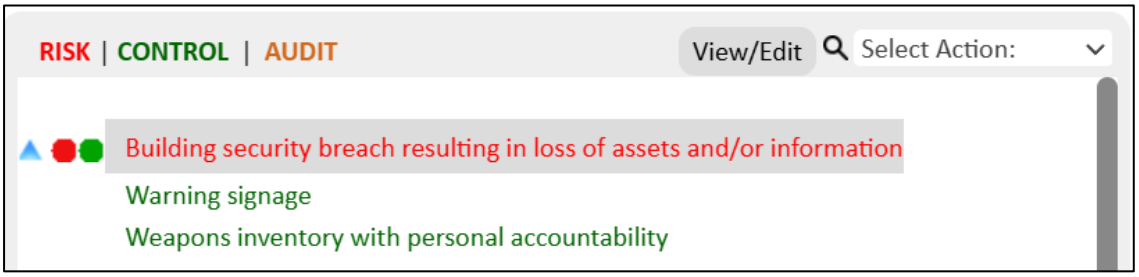
- Percentage based effectiveness ratings can be easily applied to the Inherent Risk
- This quantitative approach brings structure and transparency to an otherwise qualitative process
- Most importantly, it encourages consistent thinking about risks and controls across the organisation

RESIDUAL RISK CALCULATION

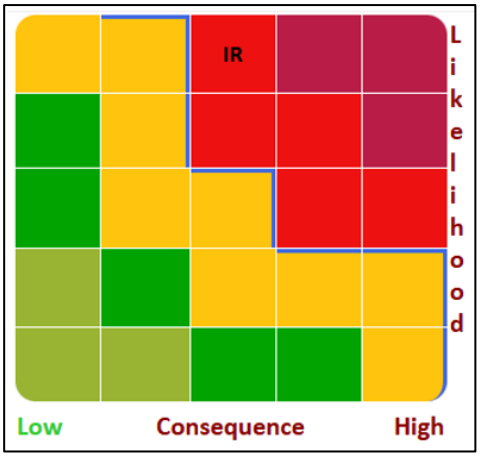
Once all controls are attached to a risk, the effectiveness scores of these controls are aggregated and applied to the Inherent Risk level to get the Residual Risk Score:

Residual Risk = Inherent Risk Level x Effective Control

Here is a worked example:



- The attached risk around Building Security has a Consequence of ***Moderate*** (3) and a Likelihood of ***Almost Certain*** (5) – resulting in an IR score of "High"



- We then attach two controls with the following effectiveness ratings

Control Name	Control Status	Effectiveness Consequence	Effectiveness Likelihood
Warning signage	Implemented	Slightly Effective	Slightly Effective
Weapons inventory with personal accountability	Implemented	Somewhat Effective	Slightly Effective

Applying our Control Effectiveness percentages, we get:

Control	Likelihood	Consequence
Warning Signage	Slightly Effective (20%)	Slightly Effective (20%)
Inventory	Slightly Effective (20%)	Somewhat Effective (40%)

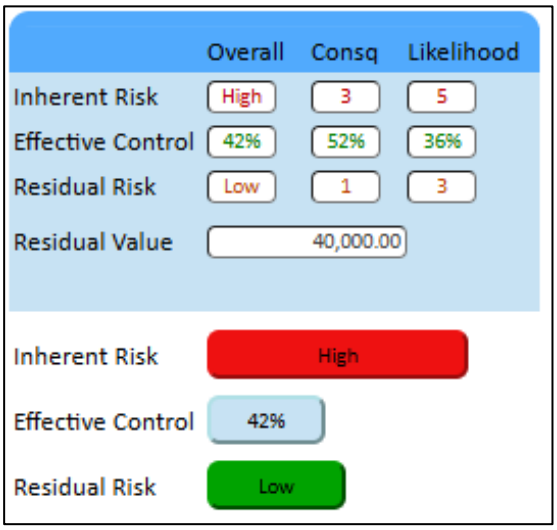
Combined Likelihood Calculation: $1 = (1 - 0.2) \times (1 - 0.2) = 1 - 0.64 =$ **36%**

Combined Consequence Calculation: $1 = (1 - 0.2) \times (1 - 0.4) = 1 - 0.48 =$ **52%**

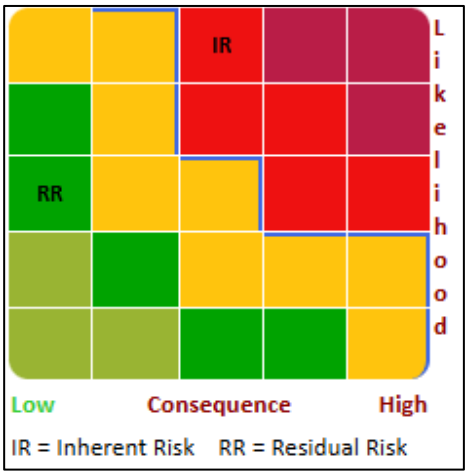
- Thus, we apply the control effectiveness calculation to the inherent risk ratings as follows:

Inherent Consequence	(3) – (3 * 0.52) = 1.44 = **1** (Rounded)
Inherent Likelihood	(5) – (5 * 0.36) = 3.20 = **3** (Rounded)

The overall score is the approximate average of both the consequence and likelihood ratings



- Therefore, the residual risk is deemed low and reflected on the risk heat map accordingly:



MANUAL RISK OVERRIDE

In the event that a user disagrees with the residual risk rating (potentially considered too low) – GuardianERM has a *"residual risk manual override"* button within the ***Risk Evaluation Details*** Screen.

]